Napadi na metode autentikacije i autorizacije unutar Active Directory okruženja

Miličević, Dino

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

DINO MILIČEVIĆ

NAPADI NA METODE AUTENTIKACIJE I AUTORIZACIJE UNUTAR ACTIVE DIRECTORY OKRUŽENJA

Završni rad

Pula, srpanj, 2023. godine

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

DINO MILIČEVIĆ

NAPADI NA METODE AUTENTIKACIJE I AUTORIZACIJE UNUTAR ACTIVE DIRECTORY OKRUŽENJA

Završni rad

JMB: 0297012510, redoviti student/ica
Studijski smjer: Sveučilišni preddiplomski studij Računarstva

Predmet: Programsko inženjerstvo
Znanstveno područje: Tehničke znanosti
Znanstveno polje: Računarstvo
Znanstvena grana: Programsko inženjerstvo
Mentor: prof.dr.sc. Tihana Galinac Grbac

Pula, srpanj, 2023. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Dino Miličević, kandidat za prvostupnika, smjera Računarstva ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, Dino Miličević dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Napadi na metode autentikacije i autorizacije unutar Active Directory okruženja, koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj

1. Uvod

Microsoft Active Directory (Microsoft, 2022)[1] (u nastavku AD) je programsko rješenje za nadzor, upravljanje i orkestraciju resursa u organizacijskom okruženju. Zbog svoje efikasnosti, olakšane upravljivosti kroz grafičko sučelje te odlične integracije sa široko rasprostranjenim Windows računalima (Krishnamoorthi & Carleton, 2020)[2], iznimno je popularno u današnjim tvrtkama – oko 90% *Fortune 1000* organizacija koristi AD kao glavno rješenje za upravljanje svojim računalnim entitetima, poput računala, printera, korisnika i slično. Obzirom na svoju popularnost i zastupljenost u velikim tvrtkama, AD je također dobro poznata meta i kibernetičkim kriminalcima (Smith, 2023)[3] koji iskorištavaju ranjivosti u samom alatu ili (češće) pogrešne konfiguracije ovog alata kako bi ostvarili financijsku odnosno informacijsku dobit, ili nanijeli reputacijsku štetu nekoj organizaciji.

Ovaj rad će predstaviti osnovne koncepte i arhitekturu sustava upravljanog pomoću Active Directory alata, tipične miskonfiguracije takvog sustava te će donijeti pregled osnovnih napada na ova okruženja. Isto tako, kroz rad će se prikazati korištenje određenih ofenzivnih alata sa strane kibernetičke sigurnosti i artefakti koje napadi ostavljaju kako bi se mogli identificirati indikatori kompromisa (engl. *Indicators of Compromise, IoC*) u svrhu razvoja metoda detekcije i/ili prevencije ovakvih napada.

Za potrebe demonstracije podignuto je virtualno testno okruženje u kojem se nalazi jedan *Domain Controller*, jedno obično korisničko računalo i Kali računalo koje će se koristiti kao pomoćno računalo za napad na sustav. Korisnici u sustavu su *dmilicevic* koji predstavlja običnog korisnika s niskim privilegijama te *DA-dmilicevic* koji predstavlja adminstratora domene (engl. *Domain Administrator*).

---

[1] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
[2] https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/
[3] https://petri.com/cyberattacks-increased-38-in-2022-secure-active-directory-now/

2. Active directory

2.1 Povijesni pregled

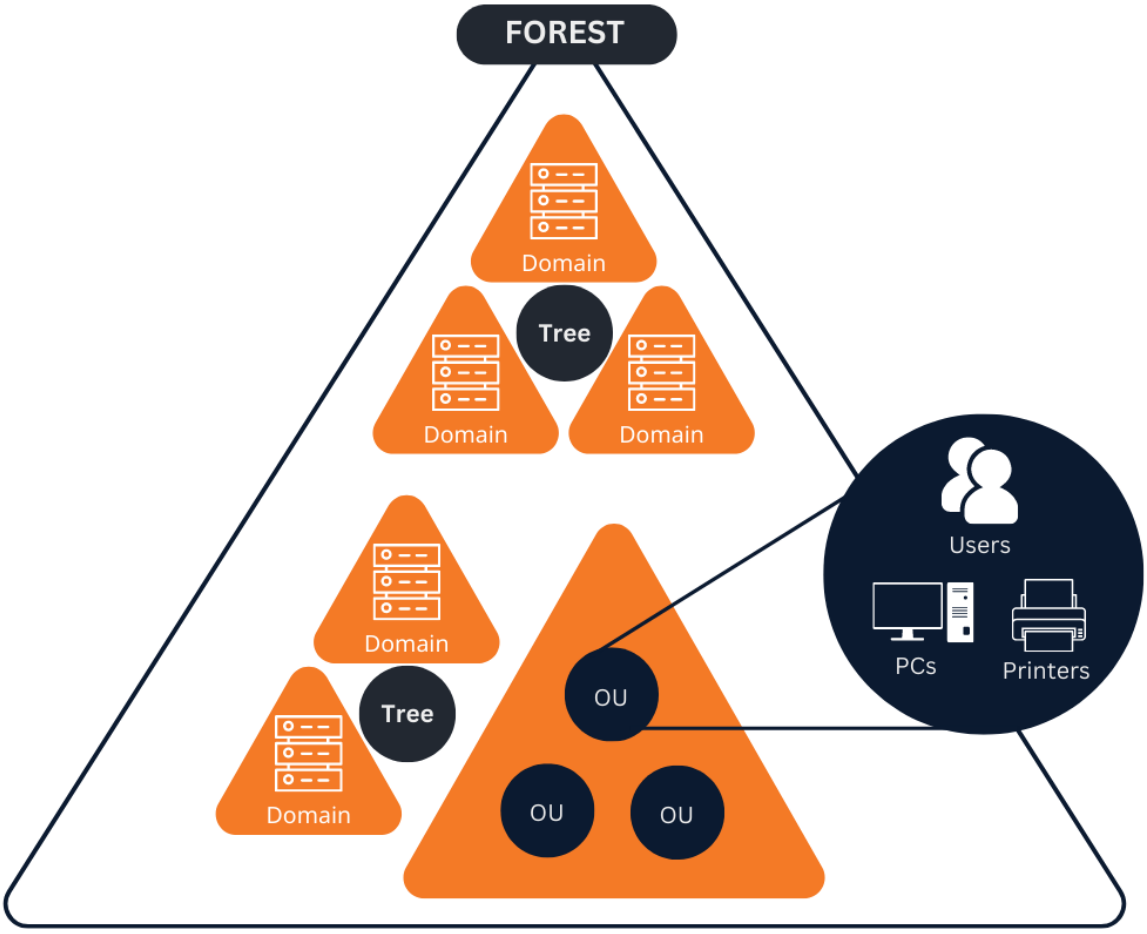
Microsoft Active Directory je proizvod koji je povijesno značajan za tvrtku Microsoft i koji donosi velike promjene u upravljanju mrežnih sustava. Active Directory je predstavljen zajedno s Windows serverom 2000. godine. (Desmond, Richards, Allen, & Lowe-Norris, 2013)[4] Prije nastanka AD-a, Microsoftovo rješenje za upravljanje korisnicima i resursima su bile Windows NT domene. Ove domene su bile decentralizirane, što je značilo da je svaka domena imala isključivo svoju bazu podataka i nije imala uvid u druge domene, iako su se one mogle nalaziti u istoj mreži. Samim time, Windows NT domene su bile ograničene s gledišta skalabilnosti jer nisu bile prikladne za korištenje u modernim sustavima koji su često iznimno granularni, podijeljeni na logičke odnosno semantičke cjeline te se potencijalno protežu na nekoliko kontinenata. Izlaskom poslužiteljskog izdanja *Windows 2000* operacijskog sustava na tehnološku scenu stupa i Active Directory te ubrzo postaje dominantno rješenje za upravljanje mrežnim sustavima. AD donosi hijerarhijsku strukturu za organiziranje objekata, kao što su korisnici, računala i grupe, unutar takozvanih *domena*, *drveća* (engl. *Tree*), odnosno *šuma* (engl. F*orest*). Ovakva hijerarhijska struktura postavila je drukčiji standard upravljanja sustavom, ali je ujedno i težila za poboljšanjima u području sigurnosti i performansi.

Dolaskom *Windows Server 2003* i *Windows Server 2008* operacijskih sustava dolaze i navedena poboljšanja sigurnosnih aspekata i efikasnosti. Također je uvedena i podrška za više domena unutar jednog AD sustava, podrška za migraciju starih NT domena na moderne AD domene, dodatak za lakše upravljanje resursima unutar sustava u obliku *Domain Services* uloge (engl. *Domain Services Role*) te podrška za *forest*. U novijim verzijama, AD donosi implementacije novih sigurnosnih mehanizama poput korištenja jednokratnih lozinki i višefaktorske autentifikacije, kao i podršku za moderna okruženja u oblaku (engl. *cloud*) u obliku *Azure Active Directory* web aplikacije. Ovim koracima

[4] 2013, Desmond, Brian; Richards, Joe; Allen, Robbie; Lowe-Norris, Alistair G., Active Directory, 4th Edition, O'Reilly

Microsoft pospješuje integraciju svih svojih proizvoda u jedan sustav, dozvoljavajući i hibridne modele u kojima korisnici mogu djelomično koristiti i vlastite poslužitelje (engl. *on-premise infrastructure*) uz dostupne *cloud* alternative. Također, jača povezanost s ostalim Microsoft alatima, poput cijelog *Office365* (odnosno danas *Microsoft 365*) paketa alata, Microsoft Defender EDR (engl. *Endpoint Detection and Response*) rješenjem, i mnogim drugima. (Microsoft, 2023)[5]

Slika 1. Arhitektura Active Directory okruženja



https://redfoxsec.com/blog/active-directory-basics/

2.2 Glavne funkcionalnosti i principi rada

[5] https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Sve resurse unutar nekog Active Directory okruženja nazivamo objektima te ih možemo svrstati u 2 glavne grupe: kontejnerski objekti i listovi. Svaki od ovih tipova objekata izvršava odnosno služi određenoj funkcionalnosti, stoga su tako i semantički raspodijeljeni. (Microsoft, 2022)[6]

2.2.1 Korisnički račun

Korisnički račun (engl. *User*) je rubni objekt (list) koji sadrži informacije o stvarnom korisniku sustava kojem je dodijeljena lozinka i korisničko ime, jedinstveni identifikator, telefonski broj i drugi atributi. Ovaj objekt može imati hijerarhijski nadređenog korisnika (primjerice voditelj tima), može biti član raznih grupa na temelju kojih mu se mogu dodjeljivati razne ovlasti te se može aktivno prijavljivati u sustav koristeći svoje vjerodajnice.

2.2.2 Kontakt

Kontakt (engl. *Contact Object*) je tip rubnog objekta koji sadrži atribute slične korisničkom računu, no ne može se aktivno prijavljivati u sustav. Svrha kontakta jest da služi kao referenca na vanjske korisnike odnosno suradnike te da sprema informacije o njima ukoliko one budu potrebne, analogno telefonskom imeniku ili posjetnici.

2.2.3 Računalo

Računalo (engl. *Computer Object*) je list koji predstavlja računalo koje je spojeno u neku AD domenu. Sadrži razne atribute poput jedinstvenog identifikatora, DNS naziva, verzije operacijskog sustava i slično te, poput korisničkog računa, može aktivno sudjelovati u organizaciji.

[6] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

2.2.4 Grupa

Grupa (engl. *Group*) u Active Directoryju predstavlja kontejner unutar kojeg se mogu nalaziti drugi objekti poput korisnika, računala, kontakata ili drugih grupa te se dodatno dijele na 2 glavna tipa: sigurnosne grupe i distribucijske liste.

Sigurnosne grupe (engl. *security group*) su kontejneri koji se koriste kako bi se putem njih određenim objektima dodijelila određena prava. Primjerice, jedna od pretpostavljenih sigurnosnih grupa u Active Directory sustavu je grupa *Domain Administrators* – svi korisnici ove grupe imaju vrhovna prava nad nekom AD domenom.

S druge strane, distribucijske grupe (engl. *distribution group*) su grupe koje se koriste u svrhu jednostavnijeg razašiljanja e-mail poruka njenim članovima. Primjerice, moguće je kreirati jednu grupu naziva *Zavod za matematiku* kojoj je dodijeljena e-mail adresa *matematika[at]unipu.hr*, a unutar koje se dodatno nalaze distribucijske grupe za pojedine matematičke predmete na sveučilištu. Kada netko pošalje e-mail na navedenu adresu, svi će članovi distribucijske grupe (bilo direktni ili indirektni, primjerice članovi ugnježđenih grupa) primiti tu poruku.

Uz navedene objekte postoje i dodatni tipovi resursa – neki od njih su manje bitni pa ih se u ovom radu neće dodatno opisivati (npr. dijeljene mape, printeri i slično), dok su neki od njih direktno vezani uz strukturu cijelog Active Directory sustava te će se detaljno objasniti u nastavku.

2.3 Hijerarhijska struktura

Struktura Active Directory sustava je slična strukturi Windows datotečnog sustava (NTFS, *New Technology File System*) – dozvoljava grupiranje elemenata u stablastu strukturu koja ima jedan ili više korijena (*forest*), ispod kojeg se nalazi mnoštvo drugih elemenata, počevši s *Tree* odnosno *Domain* elementom, a završavajući s nekim od rubnih objekata (ili praznim kontejnerom) kao listovima stabla.

2.3.1 Domena

Domena (engl. *domain*) je logička organizacijska jedinica koja omogućuje centralizirano upravljanje korisnicima, računalima i drugim objektima u mrežnom okruženju. Predstavlja osnovnu jedinicu administracije i omogućuje organizaciju i upravljanje resursima na mreži. Primarna svrha joj je logičko grupiranje korisnika, računala i drugih objekata prema potrebi administracije i sigurnosti. Stoga je, primjerice, uobičajena praksa kreirati zasebne domene za testna, produkcijska, i druga okruženja. Glavnu ulogu u administriranju pojedine domene imaju korisnici s ulogom *Domain Administrator.*

Active directory domena je servis koji omogućuje centraliziranu administraciju svih radnih stanica i servera na bilo kojem sustavu. Zbog široke upotrebe i usvajanja ove usluge, postala je meta mnogih napadača. Napadi na Active Directory razvijali su se godinama. Napadi ciljaju različite funkcije i značajke koje pruža Active Directory. U nastavku objašnjavanjem administracije govorimo o konceptu Active Directory sustava i objašnjavamo tri vrste napada i različite mehanizme obrane.[7] *(Mokhtar, 2022).*

Domena unutar AD sustava sastoji se od četiri glavne komponente: hijerarhijske strukture kontejnera i rubnih objekata, jedinstvnog imena domene (analogno internetskim domenama, „identifikator“), politike ponašanja (engl. *Group Policy*) te sigurnosnih elemenata koji omogućuju autentifikaciju i autorizaciju entiteta domene. O ovim elementima će se detaljno pričati tijekom ovog rada.

Važno je napomenuti da se ime domene koristi i u kontekstu DNS protokola kako bi se pojedina računala unutar domene mogla identificirati putem njihovog naziva umjesto IP adrese. Primjerice, web server unutar AD domene „*domena.local*“ možemo nazvati „*web01“*, što znači da će domenski DNS poslužitelji moći identificirati IP adresu tog računala ukoliko se pošalje DNS upit za „*web01.domena.local*“. Upravo iz ovog razloga, preporučeno je korištenje privatnih TLD ekstenzija (*top-level domain*) poput *.local, .lab* ili

[7] Mokhtar, Basem & Jurcut, Anca & ElSayed, Mahmoud & Azer, Marianne. (2022). Active Directory Attacks—Steps, Types, and Signatures. Electronics.

sličnih, kako se interna domena ne bi slučajno podudarala s javnom, internetskom domenom što u nekim slučajevima može dovesti do značajnih sigurnosnih propusta.

2.3.2 Stablo

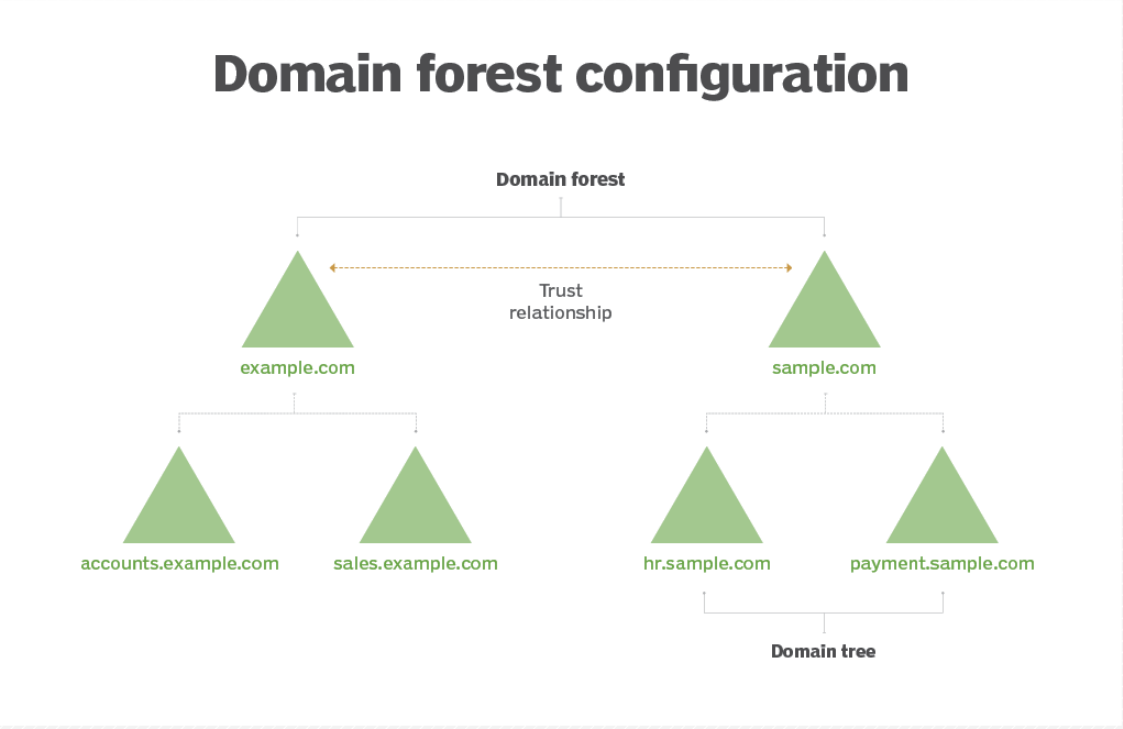
Ukratko, stablo (engl. t*ree*) je grupacija više poddomena jedne domene koje međusobno mogu pristupati resursima domene roditelja ili susjednih poddomena zahvaljujući konceptu „vjerovanja“ (engl. *trust*) – ukoliko jedna domena „vjeruje“ drugoj, odnosno uspostavljen je *trust* između njih, korisnici u pojedinoj domeni će moći koristiti resurse iz druge. Kako bi ovaj *trust* pravilno funkcionirao, potreban je *Global Catalog* poslužitelj (ujedno i *Domain Controller*) koji sadrži informacije o svim resursima u stablu.

2.3.3 Šuma

U AD sustavu, šuma (engl. *forest*) označava jednu ili skupinu domena koje djeluju kao jedna cjelina, primjerice jedna organizacija može biti smještena unutar jedne šume. *Forest* je najviša razina hijerarhije u Active Directoryju, ima jedinstveno, nepromjenjivo ime i stablo DNS imena koji koristimo za identifikaciju svih objekata u šumi. Glavnu ulogu u administriranju pojedine šume imaju korisnici s ulogom *Enterprise Administrator.*

Prilikom kreacije šume, sve domene koje šuma obuhvaća će uspostaviti implicitni *trust*, no dvije šume si međusobno neće vjerovati osim ako se takav *trust* model eksplicitno ne kreira. Ovakav model korištenja većeg broja šuma je česta praksa u velikim organizacijama koje su interno razdvojene geografski i/ili logički što omogućuje bolju semantičku odvojenost, no isto tako potencijalno unosi nove sigurnosne probleme koji izlaze van okvira ovog rada.

Slika 2. Odnos domena, stabla i šume

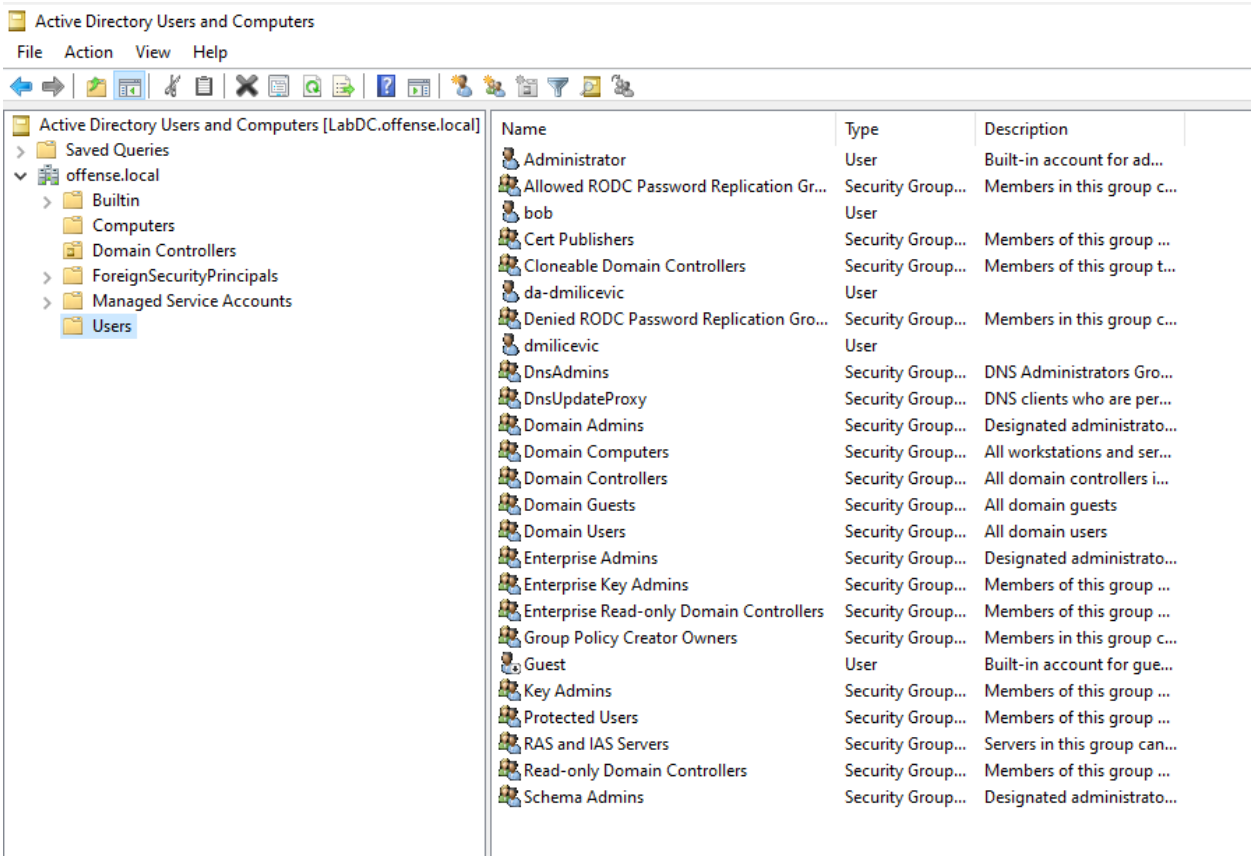


https://www.techtarget.com/searchwindowsserver/definition/Active-Directory-tree-AD-tree

2.3.4 Organizacijska jedinica

Organizacijske jedinice (engl. *organizational unit, OU*) su kontejneri koji služe za logičko odvajanje elemenata domene. Primjerice, uobičajena je praksa kreirati zasebne OU na temelju geolokacije, pojedinih odjela unutar organizacije i slično. OU kontejner osim rubnih objekata također može sadržavati i druge OU, što dozvoljava granularnije razdvajanje pojedinih entiteta unutar domene. Primjerice, kako bismo razdvojili klijentska od poslužiteljskih računala, možemo kreirati OU „*računala*“ unutar kojeg se nalaze dodatna 2 OU kontejnera „*klijenti*“ i „*poslužitelji*“. Također, nad pojedine organizacijske jedinice moguće je primijeniti prilagođene politike ponašanja kako bi se određenim objektima ograničila prava na samo one resurse koji su im potrebni.

Slika 3. Primjer strukture Active Directory sustava



Microsoft je razvio hijerarhijsku strukturu da pruži uslugu koja se odnosi na pohranu informacija o objektima putem opsežnog popisa objekata na mreži. Mrežni administratori kreiraju i upravljaju korisnicima i objektima unutar dane mreže što zauzvrat zahtijeva organizaciju mreže na pravilan način. Kako mreža raste, potrebno je veliki broj korisnika organizirati u logičke grupe i podgrupe, uz osiguranje kontrole pristupa na svakoj razini, što zahtijeva korištenje Active Directoryja. Microsoft je razvio hijerarhijsku strukturu kako bi dao uslugu koja se odnosi na pohranjivanje informacija o objektima putem sveobuhvatnog popisa objekata na mreži. (Iyer, 2020).

2.3.5 Politike ponašanja

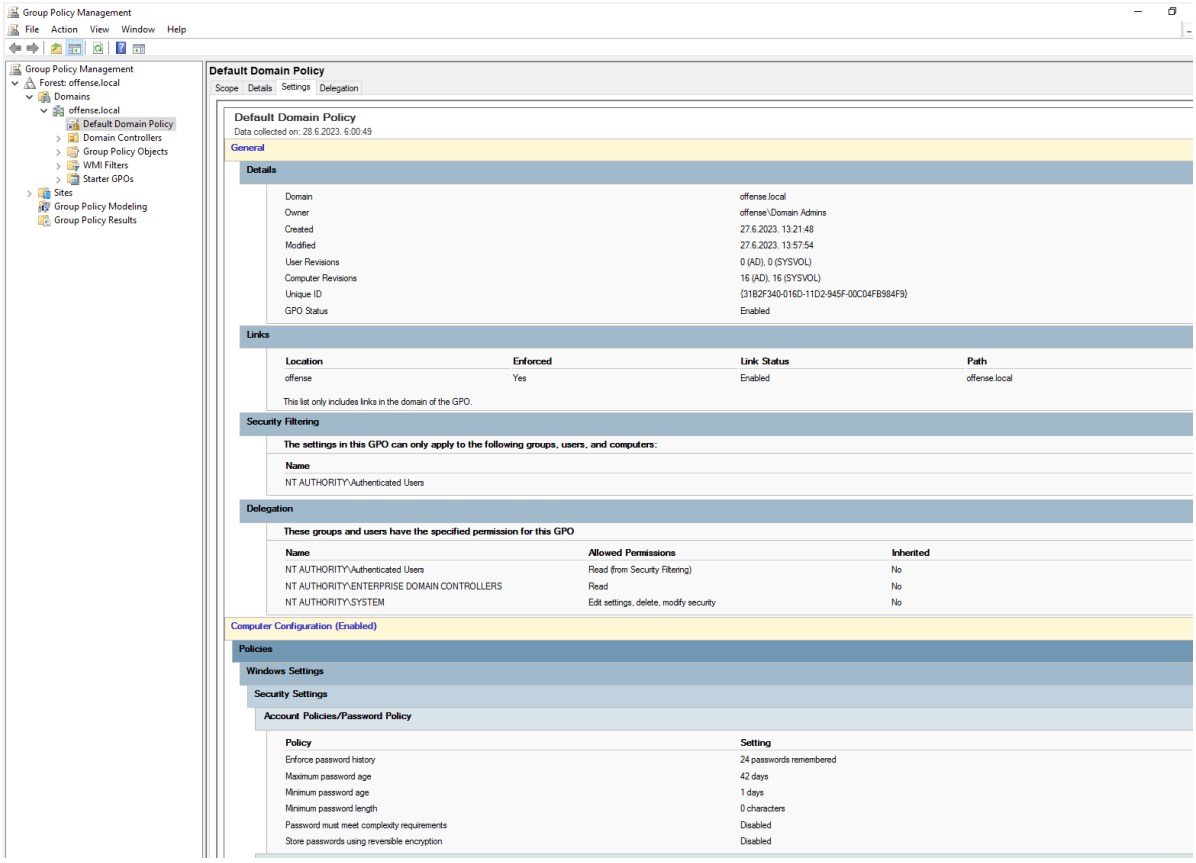
Kako bi se omogućila granularnost upravljanja resursima nekog AD sustava, kreirane su politike ponašanja, odnosno *Group Policy Objects (GPO)*. GPO je tip objekta koji administratoru dozvoljava da provede željene politike nad računalima i korisnicima kako bi ih prisilio da se ponašaju u skladu s pravilima sustava. Neke od često korištenih politika uključuju postavljanje minimalne kompleksnosti lozinke, prisilno omogućavanje

Windows Update funkcionalnosti, zabrana promjene lokalnih sigurnosnih postavki (primjerice zaustavljanje antivirusnog rješenja) i slično. Ove politike se mogu primijeniti na razini organizacijske jedinice, domene, stabla ili šume, a skladnost pojedinog resursa i primijenjene politike se osigurava sinkronizacijskim mehanizmima koji se periodički i automatizirano primjenjuju na resurse.

Važno je za spomenuti da se politike koje se primjenjuju na resurs uvijek primjenjuju definiranim redoslijedom, poznatim pod skraćenicom *LSDOU – Local, Site, Domain, Organizational Unit.* Ovo znači da se prvo primjenjuju lokalne politike resursa, zatim politike definirane nad nekim AD *site*-om (internetska mreža koja definira fizičku strukturu AD-a), politike nad domenom i konačno politike nad nekom organizacijskom jedinicom. Ukoliko se neki dijelovi politika preklapaju, primjenjuje se ona koja dolazi kasnije u lancu, odnosno politika definirana nad OU objektom će uvijek biti primjenjena.[8]

[8] Iyer, Nalini & Kabbur, Anil & Wali, Heera. (2020). Implementation of Active Directory for efficient management of networks. Procedia Computer Science.

Slika 4. Group Policy Objects



2.4 Vrste poslužitelja

Obzirom na širok spektar funkcionalnosti koje su dostupne kao dio Active Directory sustava, uobičajena je praksa kreirati razdvojene poslužitelje za različite funkcionalnosti. Neki od bitnijih poslužitelja koji se nalaze u većini Active Directory okruženja su *Domain Controller (DC)*, NPS, DNS, VPN poslužitelji i mnogi drugi.

2.4.1 Domain Controller

Domain Controller (DC) je glavni autentikacijski i autorizacijski poslužitelj u AD sustavu. Služi kao baza podataka koja sadrži informacije o svim resursima koji se nalaze u njegovoj domeni uključujući i korisničke podatke te ostale konfiguracijske datoteke potrebne za očuvanje strukture Active Directoryja. Ovaj poslužitelj također često poprima i ulogu DNS poslužitelja. Jedna od najvažnijih datoteka na svakom *Domain Controller* poslužitelju je *NTDS.dit* (*New Technology Directory Services*) datoteka koja

sadrži osjetljive informacije o korisnicima, poput njihovih korisničkih imena, lozinki, pripadnosti grupama i slično. Upravo zbog svog sadržaja, *NTDS.dit* je jedna od glavnih meta napadača.

2.4.2 Replikacija

Obzirom da je DC glavni autentifikacijski i autorizacijski poslužitelj, nužno je ovaj poslužitelj održati stabilnim i aktivnim. Kako bi se osigurala mogućnost *failover*-a, odnosno korištenje zamjenskog poslužitelja u slučaju kvara, u AD okruženjima se nerijetko instalira nekoliko DC poslužitelja. Kako bi podaci na različitim DC-ovima bili konzistentni, uveden je mehanizam replikacije podataka koji putem RPC protokola sinkronizira informacije među DC poslužiteljima. Obzirom da se tijekom ovog procesa prenose osjetljive informacije, razvijene su napadačke metode za izvlačenje podataka koristeći ovaj mehanizam, primarno u obliku *DC Sync* napada.

2.4.3 Network Policy Server

NPS poslužitelj u Active Directory sustavu služi za autentifikaciju i autorizaciju korisnika prilikom pristupa mrežnim resursima u okruženju. NPS omogućuje administratorima da granularno kontroliraju pristup određenim dijelovima mreže, ovisno o pravima korisnika, uređaju ili lokaciji s koje se spajaju i slično. U svojim temeljima, NPS poslužitelj je zapravo Microsoftova implementacija protokola RADIUS (*Remote Authentication Dial-In User Service*), koji u suradnji s podacima iz Active Directoryja donosi odluke o autorizaciji i autentifikaciji korisnika na mrežu.

2.4.4 Domain Name Service

DNS poslužitelj je ključni dio infrastrukture AD-a jer omogućuje prevođenje imena domena u IP adrese i obrnuto. Ovi poslužitelji osiguravaju pravilan rad usluga u sustavu i omogućuju ispravnu komunikaciju klijenata i poslužitelja, analogno internetskim DNS poslužiteljima. DNS unutar AD-a možemo smatrati i integriranim DNS poslužiteljem jer koristi AD za pohranu informacija o DNS zapisima. Prednosti AD DNS-a su brojne, a jedna od njih je i konzistentnost između podataka AD-a i DNS podataka, njihovo

repliciranje i slično. Česta je praksa kao glavne DNS poslužitelje za sustav koristiti *Domain Controller*-e, koji u slučaju nepoznatog zahtjeva isti prosljeđuju dalje, do glavnog (engl. *primary*) DNS DC poslužitelja, koji će u tom slučaju ili vratiti odgovor na upit, ili ga proslijediti nekom vanjskom DNS poslužitelju, poput Google-a. Ovaj model je također poznat kao *DNS Forwarding*.

2.4.5 VPN

VPN poslužitelj unutar Active Directory okruženja pruža siguran i privatan pristup korporativnom mrežnom okruženju putem Interneta. VPN poslužitelj integriran je s AD-om te ga koristi za autentifikaciju korisnika na lokalnu mrežu. Administratori mogu postavljati pravila za pristup VPN-u i ograničiti pristup određenim grupama korisnika te pratiti i nadzirati aktivnost za udaljene korisnike koji mogu raditi i izvan fizičkog prostora ureda. Bitno je za primijetiti da, obzirom na prirodu ovog poslužitelja, VPN servis mora biti objavljen na javnom Internetu, što znači da ovaj poslužitelj mora biti redovno ažuriran te kvalitetno osiguran i nadziran koristeći alate poput vatrozida i IPS rješenja (engl. *Intrusion Prevention System*).

3. Azure Active Directory

Azure AD (AAD) je moderna paralela klasičnom, fizičkom (engl. *on-premises*) Active Directory okruženja koja je izgrađena u oblaku. AAD omogućuje zaposlenicima pristup vanjskim resursima, kao što su Microsoft 365, Azure portal i druge SaaS aplikacije, ali i pristup internim resursima kao što su aplikacije na korporativnom intranetu ili bilo koje interno razvijene aplikacije u oblaku. Azure AD je dizajniran kako bi omogućio organizacijama upravljanje identitetima i pristupom na vlastite *cloud* i *on-premises* resurse. Može se koristiti kao pružatelj identiteta za različite aplikacije prve i treće strane uz pomoć OAuth integracije i za upravljanje privilegijama pristupa korisnika u organizaciji kroz *Privileged Identity Management* konzolu.

Važno je napomenuti kako je Azure uklonio koncept domena odnosno šuma. Umjesto toga, AAD dodaje novi koncept koji nazivamo organizacijama (engl. *tenant*). *Tenant* je povezan sa jednim identitetom (osobom, tvrtkom ili organizacijom) i jednom instancom AAD-a te može posjedovati jednu ili više pretplata (engl. *subscriptions*) koje se nalaze u istoj instanci – slično konceptu stabla i domene. Svaka pretplata može sadržavati zasebne odnosno izolirane resurse, poput virtualnih strojeva, mrežnih kartica, prostora za pohranu i slično te će se svaka pretplata naplaćivati zasebno.

3.1 Hibridni model

Obzirom na količinu već postavljenih *on-premises* Active Directory okruženja i potencijalne troškove koje donosi migracija na *cloud* rješenje, Microsoft nudi opciju integracije postojećeg *on-premises* AD-a s *cloud* AAD-om. Ova integracija omogućuje organizacijama da koriste iste identitete za pristup lokalnim i cloud resursima, stvarajući jedinstveno korisničko iskustvo i olakšavajući upravljanje identitetima.

Jedna od glavnih prednosti hibridnih modela Azure AD-a je mogućnost korisnika da imaju jedno korisničko ime i lozinku za pristup različitim aplikacijama i resursima, bez obzira na to jesu li smješteni lokalno ili u oblaku, što se postiže pomoću servisa kao što su *Azure AD Connect* i *Active Directory Federation Services (ADFS)*, koji omogućuju sinkronizaciju korisničkih računa, grupa i atributa iz lokalnog AD-a u Azure AD. Dodatno, uvođenje AAD-a olakšava implementaciju višefaktorske autentifikacije, nadzor korisničkih prijava, promjena nad resursima i slično.

4. Autentifikacija, autorizacija, računovodstvo

Kao moderni standard za upravljanje korisničkim računima odnosno identitetima uveden je tzv. *Triple A* model – *Authentication, Authorization, Accounting* (Aruba Networks)[9]. Ovaj model sjedinjuje proces autentifikacije (*postoji li korisnik*) i autorizacije (*posjeduje li korisnik dovoljna prava pristupa*) s računovodstvom, to jest vođenjem zapisničkih

[9]https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm

dnevnika o ponašanju korisnika, kako bi se svaki pristup resursima i sustavu pravilno regulirao i dokumentirao.

U slučaju Windows sustava odnosno specifično *on-premises* Active Directory okruženja, autentifikacija je implementirana koristeći protokole NTLM (Microsoft, 2022)[10] i Kerberos (Microsoft, 2021)[11], autorizacija se rješava koristeći pristupne liste (Medhi)[12], dok se *Event Tracing for Windows (ETW)* (Microsoft, 2021)[13] sustav brine o računovodstvu.

4.1 NTLM autentifkacija

NTLM je autentifikacijski protokol koji radi na principu *pitanje-odgovor* (engl. *challenge-response*) kako bi korisnika autentificirao u sustav. Iako se ovaj protokol smatra slabim i ranjivim, primarno zbog korištenja slabih kriptografskih metoda poput DES-a, još uvijek je relevantan i u modernim Windows sustavima zbog kompatibilnosti sa starijim verzijama operacijskog sustava.

Slično modernijem Kerberosu, NTLM protokol ima „trokutastu“ arhitekturu: u procesu sudjeluju autentifikacijski klijent odnosno korisnik, poslužitelj na kojeg se korisnik prijavljuje i autentifikacijski servis. U slučaju NTLM-a, ulogu servisa preuzima direktno *Domain Controller*.

4.1.1 Proces autentifikacije

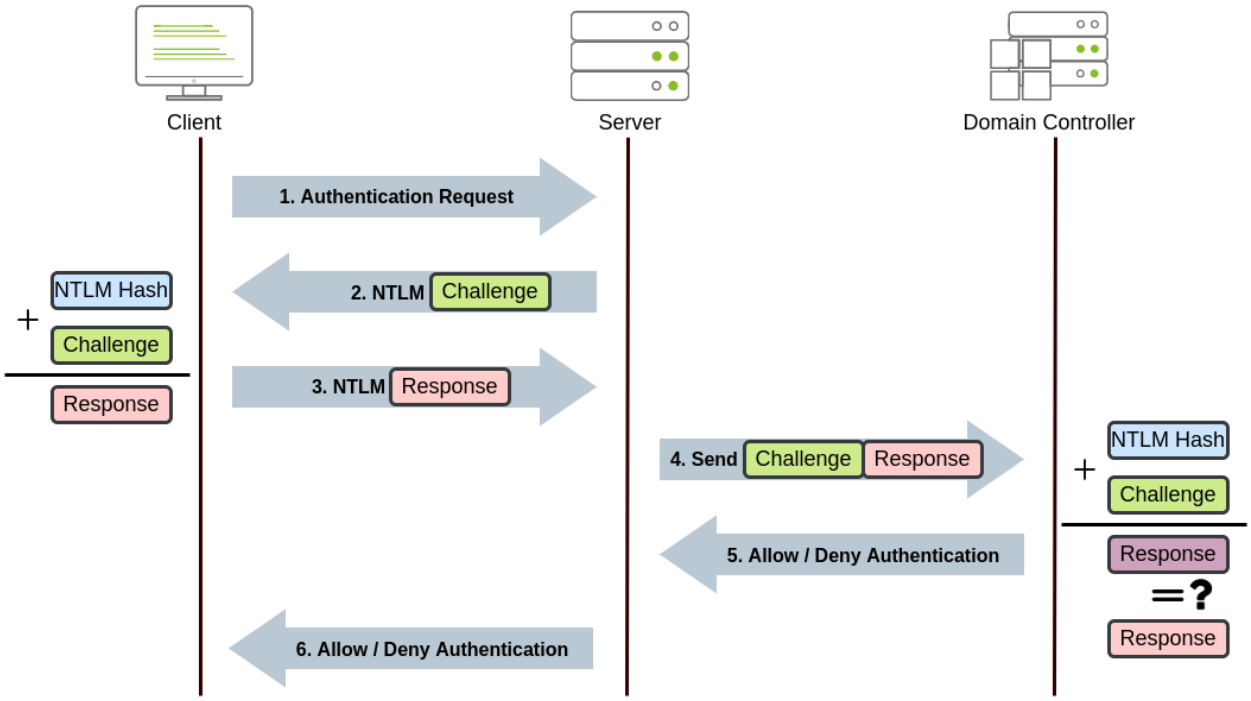
Sam proces NTLM autentifikacije može se podijeliti na sljedećih 8 koraka:

1. Korisnik prosljeđuje svoje korisničko ime, lozinku i ime domene svom lokalnom klijentu
2. Klijent kreira sažetak lozinke i briše originalnu lozinku
3. Klijent prosljeđuje korisničko ime poslužitelju na kojeg se prijavljuje
4. Poslužitelj odgovara s „pitanjem“ (*challenge*) – nasumičnim brojem od 16 bajtova

[10] https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview
[11] https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview
[12] https://www.securew2.com/blog/windows-access-control-acl-dacl-sacl-ace
[13] https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/event-tracing-for-windows--etw-

5. Klijent šifrira *challenge* sažetkom lozinke te to šalje kao odgovor (*response*) poslužitelju
6. Poslužitelj prosljeđuje *challenge*, *response* i korisničko ime prema DC-u
7. DC dohvaća sažetak lozinke iz baze i pomoću nje šifrira *challenge*
8. Na temelju usporedbe generiranog i dobivenog *response* podatka dozvoljava odnosno zabranjuje autentifikaciju korisnika u sustav. (Crowdstrike, 2023)[14]

Slika 5. Tijek NTLM autentifikacije



https://tryhackme.com/room/winadbasics

Vrijedi spomenuti da postoje 2 verzije NTLM protokola: *NTLMv1* i *NTLMv2*, koje su konceptualno jednake, no *NTLMv2* koristi snažnije kriptografske algoritme kako bi šifrirala podatke tijekom procesa. (Gombos, 2018)[15]

NTLMv1 response primjer:

[14] https://www.crowdstrike.com/cybersecurity-101/ntlm-windows-new-technology-lan-manager/
[15] https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4

```
SERVER$::DOMAIN:F35A3FE17DCB31F9BE8A8004B3F310C150AFA36195554972:F35A3FE17DCB31F9BE8A
8004B3F310C150AFA36195554972:1122334455667788
```

NTLMv2 response primjer:

```
admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310
000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c78
3030
```

4.1.2 Lan Manager sažetak

Lan Manager (LM) je najstariji tip sažetka kojeg je Windows OS aktivno koristio, kreiran u 1980.-ima. Obzirom da se izgrađuje od ograničenog broja znakova, jednostavno ga je pogoditi, a moguće ga je pronaći u *NTDS.dit* datoteci na *Domain Controller* poslužiteljima s operacijskim sustavima starijima od verzije *Windows Server 2008*.

Sažetak se kreira kroz 6 koraka:

1. Sva mala slova lozinke pretvore se u velika
2. Lozinku se dopuni do 14 znakova s *NULL* znakovima (*null-byte*)
3. Podijelimo lozinku na dvije grupe po 7 znakova
4. Svaka grupa od 7 znakova predstavlja jedan DES ključ
5. DES algoritmom šifriramo niz „KGS!@#$%“ koristeći generirane ključeve
6. Spojimo dva DES šifrirana niza i dobijemo LM sažetak (Gombos, 2018)

Primjer LM sažetka: `aad3b435b51404eeaad3b435b51404ee`

4.1.3 NT sažetak

NT sažetak (često pogrešno zvan *NTLM hash*) je kriptografski sažetak koji se koristi u modernim Windows sustavima u svrhu autentifikacije. Slično LM sažetku, moguće ga je izvući iz *NTDS.dit* datoteke na DC poslužitelju te pomoću njega izvršiti *pass-the-hash* napad.

Ovaj sažetak generira se jednostavnim algoritmom:

1. lozinku zapišemo u *little-endian* UTF-16 formatu

2. dobiveni tekst sažmemo MD4 algoritmom što rezultira NT sažetkom (Gombos, 2018)

Primjer NT sažetka: `31d6cfe0d16ae931b73c59d7e0c089c0`

4.2 Kerberos autentifikacija

Kerberos je autentifikacijski protokol koji koristi kriptografiju tajnog ključa (simetrična kriptografija) i pouzdanu treću stranu za provjeru identiteta korisnika. Prvobitno razvijen na MIT institutu kao dio projekta *Athena* u kasnim 80-ima, Kerberos je danas zadani (engl. *default*) autorizacijski protokol koji se koristi u Windows okruženjima.

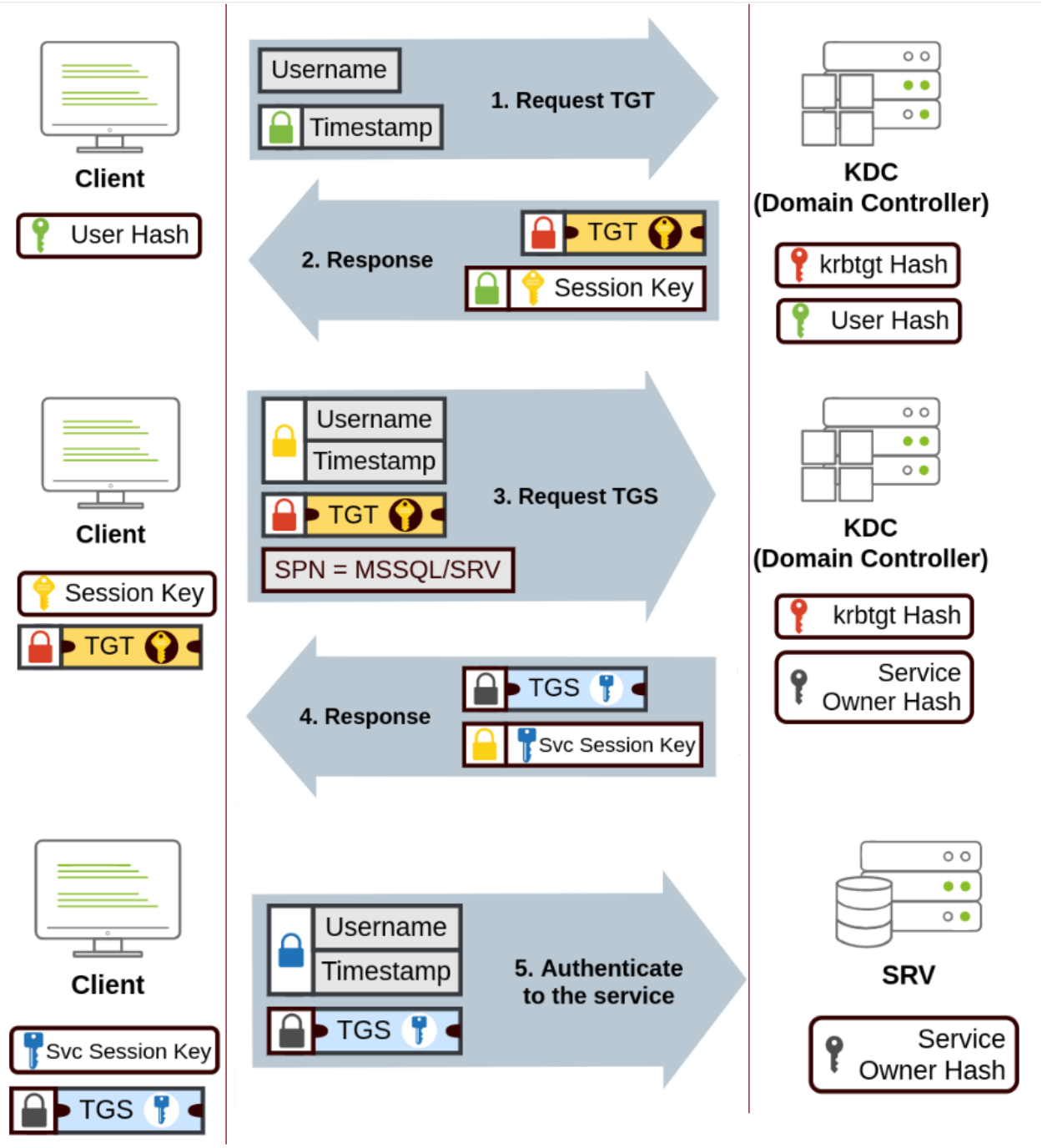
Analogno troglavom psu Kerberu iz grčke mitologije, tri „glave“ Kerberosa predstavljaju klijenta (korisnik i lokalni program), poslužitelja i centar za distribuciju ključeva (engl. *Key Distribution Center, KDC*). KDC funkcionira kao pouzdana usluga provjere autentičnosti treće strane (engl. *third-party*). Korisnici, strojevi i usluge koje koriste Kerberos ovise samo o KDC-u, koji se interno sastoji od 2 servisa: autentifikacijskog poslužitelja koji prijavljuje korisnika u sustav i servisa za izdavanje ulaznica, TGS (engl. *Ticket Granting Service*). Ulaznice su simbolički nazvani tokeni koji autentificiranom korisniku dopuštaju pristup na više resursa pokrivenih istim autentifikacijskim tijelom (u ovom slučaju, KDC unutar AD sustava). Također, slično tokenima, ulaznica ima ograničeno trajanje, što znači da svaka Kerberos ulaznica ima vremensku oznaku o izdavanju i modifikaciji te podatke o maksimalnom životnom vijeku ulaznice, nakon kojeg prestane biti važeća.

Proces autentifikacije može se raspisati u 12 koraka:

1. Korisnik lokalnom klijentu šalje korisničko ime, lozinku i domenu
2. Klijent kreira autentikacijski paket koji se sastoji od korisničkog imena, trenutnog vremena i ostalih relevantnih informacija. Svi podaci unutar ovog paketa izuzev korisničkog imena se šifriraju sažetkom korisničke lozinke.
3. Klijent šalje šifrirani paket prema KDC-u

4. KDC traži korisničko ime u svojoj bazi te (ukoliko postoji) izvlači sažetak korisničke lozinke s kojom dešifrira paket. Ukoliko dešifriranje uspije, korisnikov identitet je potvrđen. Interno, ovu radnju obavlja autentifikacijski poslužitelj (AS).
5. Nakon uspješne autentifikacije, KDC izdaje *Ticket-Granting-Ticket* (ili *Ticket-to-Give-Ticket, TGT*) koju šifrira privremenim ključem te šalje natrag korisniku. Isti privremeni ključ je podijeljen s TGS-om.
6. TGT se sprema na klijentskom uređaju te se može koristiti za pristup drugim poslužiteljima u mreži.
7. Ukoliko klijent treba pristupiti nekom drugom poslužitelju, dobiveni TGT šalje prema KDC-u (interno TGS), zajedno s identifikatorom poslužitelja kojem pristupa.
8. KDC (odnosno TGS) dešifrira ulaznicu koristeći spremljeni privremeni ključ
9. KDC (odnosno TGS) generira novu ulaznicu za pristup traženom poslužitelju, šifrira je koristeći sažetak lozinke od poslužitelja kojem se pristupa te prosljeđuje korisniku
10. Korisnik lokalno sprema novu dobivenu ulaznicu i prosljeđuje kopiju poslužitelju
11. Poslužitelj dešifrira ulaznicu koristeći sažetak svoje lozinke
12. Nakon uspješnog dešifriranja, poslužitelj provjerava svoje pristupne liste kako bi zaključio smije li propustiti korisnika (Crowdstrike, 2023)

Slika 6. Tijek Kerberos autentifikacije



https://tryhackme.com/room/winadbasics

4.3 Paswordless autentifikacija

Ova vrsta autentifikacije je najmoderniji način autentifikacije i zamjenjuje lozinke drugim faktorima provjere koje, iz perspektive korisnika, smatramo sigurnijima. Prilikom provjere autentičnosti lozinkom, lozinka koju je dao korisnik uspoređuje se s onim što je pohranjeno u bazi podataka. U *passwordless* sustavima, umjesto lozinke koriste se skeniranja lica, rožnice ili otiska prsta korisnika, FIDO sigurnosni ključevi i slične metode kako bi se na temelju ovih podataka u pozadini automatski izgenerirale vjerodajnice koje sustav povezuje s određenim korisnikom. Bitno je primijetiti da, iako ime ukazuje na drukčije, AD u pozadini još uvijek koristi lozinke za autentifikaciju korisnika kroz domenu, no u ovom slučaju tom lozinkom automatizirano upravlja sam Active Directory, ne ostavljajući korisniku na izbor duljinu i složenost lozinke. (CyberArk)[16]

Glavni nedostatak *paswordless* autentifikacije je da je relativno skupa za implementirati, zbog čega se organizacije rijetko u potpunosti prebacuju na ovaj način autentifikacije. Ako se organizacija pak odluči za korištenje *passwordless* sustava, u AD okruženju ovu mogućnost najčešće dobiju visokoprivilegirani korisnici, poput *Domain Administrator* (administrator domene) i *Enterprise Administrator* (administrator šume) uloga.

4.4 Autorizacija

Autorizacijske politike se u Windows sustavima primjenjuju kroz koncept pristupnih lista (engl. *Access Control List, ACL*). Pristupne liste se koriste kako bi se pojedinim računalima ili korisničkim računima dozvolio odnosno zabranio pristup do nekog resursa te kako bi se odredili dnevnički zapisi koji se trebaju kreirati prilikom pojedinog pokušaja pristupa. ACL-ovi se mogu podijeliti na dvije podgrupe – diskrecijske i sistemske pristupne liste.

Diskrecijske pristupne liste (engl. *Discretionary Access Control List, DACL*) su liste koje definiraju koji korisnici odnosno sigurnosne grupe imaju odnosno nemaju pravo pristupa

[16] https://www.cyberark.com/what-is/passwordless-authentication/

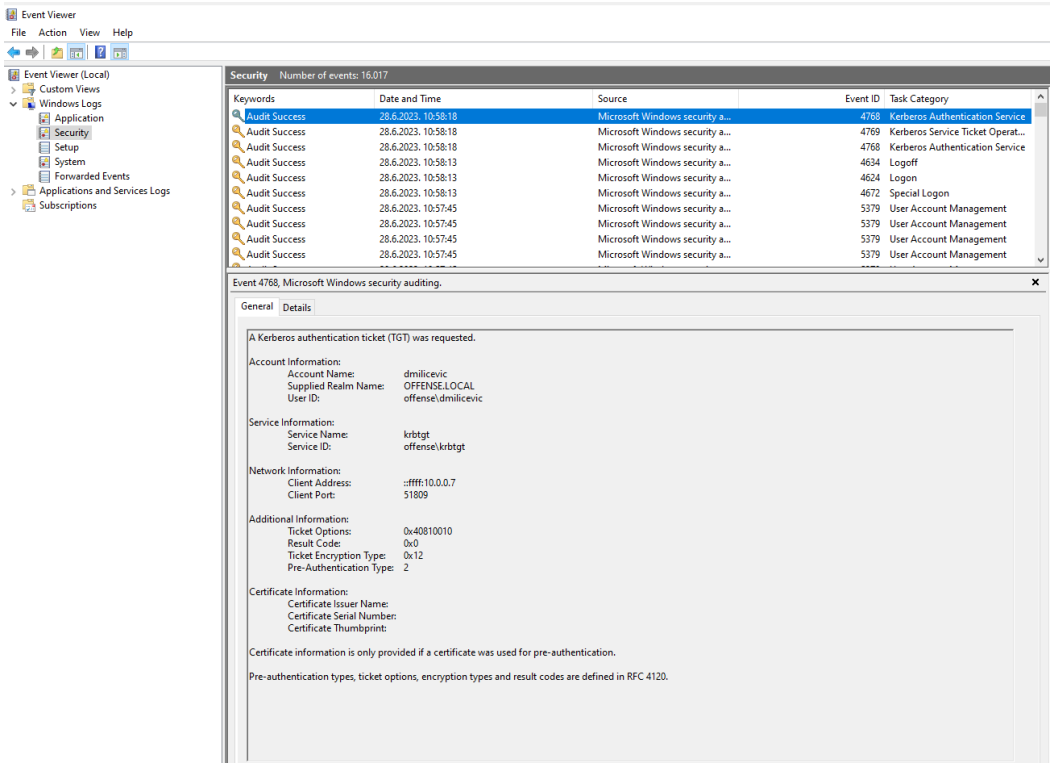
na pojedini resurs. Prilikom kreacije nekog objekta, pravo na upravljanje DACL-om se daje korisniku koji je objekt kreirao ili vlasniku objekta nad kojim je DACL kreiran.

S druge strane, sistemske pristupne liste (engl. *System Access Control List, SACL*) su liste koje definiraju događaje odnosno ponašanja korisnika koja se trebaju dogoditi kako bi se stvorio dnevnički zapis o nekom događaju. Primjerice, ukoliko neki korisnik pokuša otvoriti spomenutu *NTDS.dit*, SACL bi trebao naložiti kreiranje dnevničkog zapisa o pokušaju pristupa tom objektu. (Medhi)

4.5 Računovodstvo

Računovodstvo (*engl. Accounting)* u Windows sustavima je implementirano koristeći *Event Tracing for Windows* odnosno *ETW* servise. ETW je mehanizam koji omogućuje pouzdano praćenje događaja unutar kernela i korisničkog dijela operacijskog sustava Windows. Primarno ih dijelimo na pružatelje (engl. *providers*) i klijente (engl. *consumers*) – pružatelji su aplikacije koje osluškuju događaje unutar operacijskog sustava, a klijenti su aplikacije koji se pretplaćuju na te iste logove kako bi ih dalje koristili. Ovakvi dnevnički zapisi se u Windows operacijskom sustavu mogu vidjeti kroz *Preglednik događaja* (engl. *Event Viewer*). (Microsoft, 2021)

Slika 7. Event Viewer

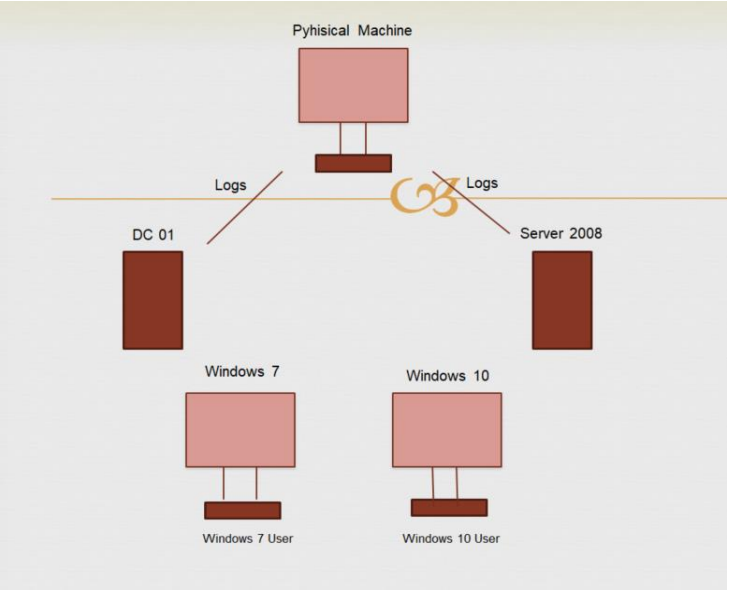


5. Napadi na NTLM autentifikacijski proces

Za izvršavanje svih vrsta napada potrebno je napraviti laboratorijsku okolinu *(engl. lab environment)* preko koje ćemo moći testirati ovu vrstu napada bez da pokušavamo oštetiti neku tvrtku ili korisnika. Da bi test bio uspješan potrebno je podići dva windows sustava koristeći virtualbox. virtualno testno okruženje u kojem se nalazi jedan *Domain Controller*, jedno obično korisničko računalo i Kali računalo koje će se koristiti kao pomoćno računalo za napad na sustav. Korisnici u sustavu su *dmilicevic* koji predstavlja običnog korisnika s niskim privilegijama te *DA-dmilicevic* koji predstavlja adminstratora domene (*engl. Domain Administrator*). Zaobilaženjem prva tri koraka autentikacije dolazimo kada uspijemo sa određenim alatima doći do ispisa sažetaka lozinki i koristimo te iste sažetke za ulogiravanje na sustav bez potrebe dodatnog pisanja lozinke. Sustavi ispod Windows 10 su imali ranjivost gdje njemu nije bila potrebna

dodatna provjera nego je sustav znao ako imamo sažetak lozinke da smo onda mi taj korisnik.[17] (Lukáš Kotlaba, 2022)

Slika 8. Lab Environment



Lukáš Kotlaba(2022)

5.1 Pass-the-Hash

Kao što samo ime govori, *Pass-the-Hash* napad se oslanja na poznavanje sažetka korisničke lozinke kako bi se napadač uspješno prijavio na sustav. Prisjetimo li se autentifikacijskog procesa NTLM protokola, lako je vidjeti da se prema poslužitelju odnosno *Domain Controller*-u ne šalje korisnička lozinka, već odgovor na *challenge* koji je šifriran NT sažetkom korisničke lozinke. Iz ovog razloga moguće se autentificirati u poznavanjem samo sažetka lozinke. (HackTricks)[18]

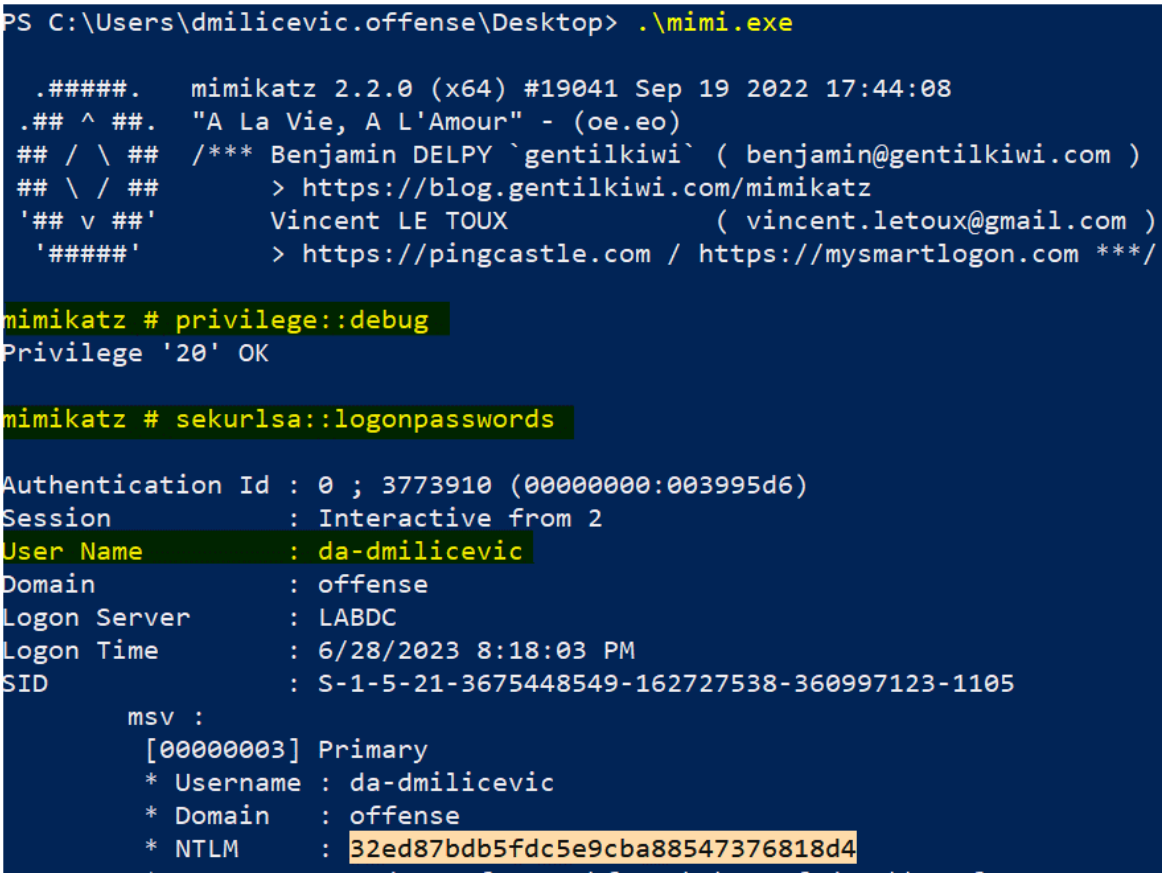
U primjeru ispod korišten je alat *mimikatz* kako bi se iz memorije žrtvinog računala izvukao sažetak lozinke – naime, prilikom prijave korisnika na računalo ili u sustav,

[17] https://pdfs.semanticscholar.org/e489/2b07da993785ab17c50cf0ddcbb3dd63db00.pdf?_gl=1*1osi83f*_ga*MTk0MjY1NjgzMC4xNjgxMjAwOTk3*_ga_H7P4ZT52H5*MTY4ODQxODE2MC44LjAuMTY4ODQxODE2MS41OS4wLjA

[18] https://book.hacktricks.xyz/welcome/readme

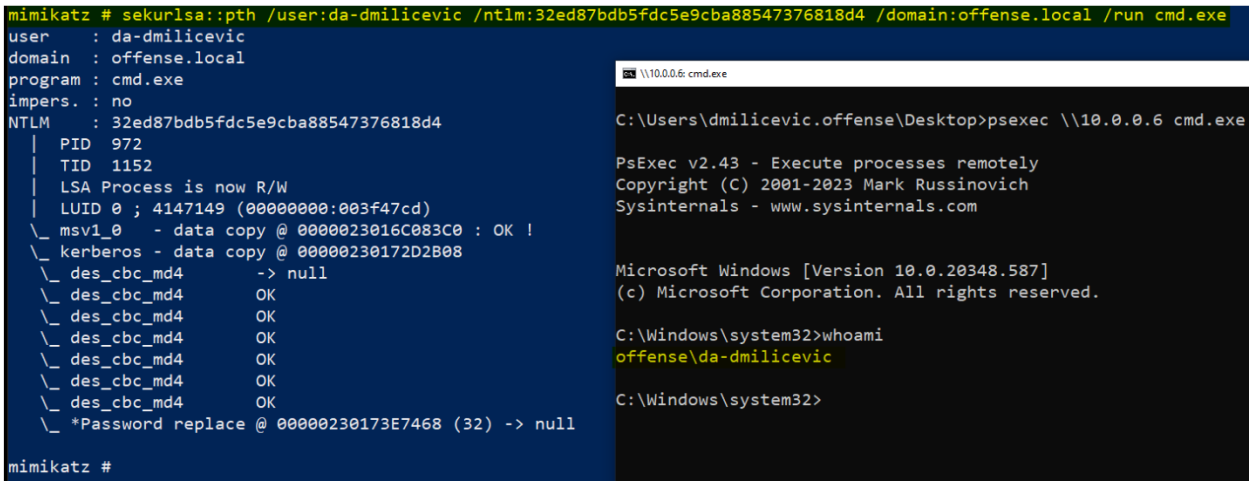
Windows u memoriju sprema sažetak lozinke u SAM (engl. *Security Account Manager*) bazu - NTHash svih prijavljenih korisnika ostaje spremljen do ponovonog pokretanja. S prilagođenim alatima poput *mimikatz*-a moguće je izvući sadržaje ove baze te zajedno s tim i NT sažetke korisničke lozinke.

Slika 9. Izvlačenje NT sažetka iz SAM baze pomoću mimikatz *alata*



Nakon što smo izvukli NT sažetak *Domain Administrator* korisnika *da-dmilicevic* koji je u jednom trenutku bio prijavljen na ovo računalo, možemo izvršiti *Pass-the-Hash* napad kako bismo s privilegijama tog korisnika mogli nastaviti napadati domenu.

Slika 10. Pokrenut Command Prompt s pravima korisnika da-dmilicevic



5.2 Overpass-the-Hash

Overpass-the-Hash je napad koji se izvodi identično kao i obični *Pass-the-Hash* napad, no interno se značajno razlikuje. Dok *Pass-the-Hash* koristi ranjivosti u NTLM protokolu kako bi se autentificirao kao neki korisnik, *Overpass-the-Hash* se oslanja na Kerberosovu kompatibilnost s NT sažetcima. Naime, korisnik se u Active Directory okruženju u kojem je onemogućena NTLM autentikacija može prijaviti koristeći svoj NT sažetak jer Kerberos prepoznaje da se radi o starom protokolu te ga automatski „modernizira“ – koristi NT sažetak umjesto lozinke kako bi pomoću nje izgenerirao *Ticket-Granting-Ticket* (TGT). Budući da je ovaj napad iznimno sličan običnom *Pass-the-Hash* napadu, nije potrebno dodatno objašnjavati metode obrane od istog. (Warren, 2022)[19]

6. Napadi na Kerberos autentikaciju

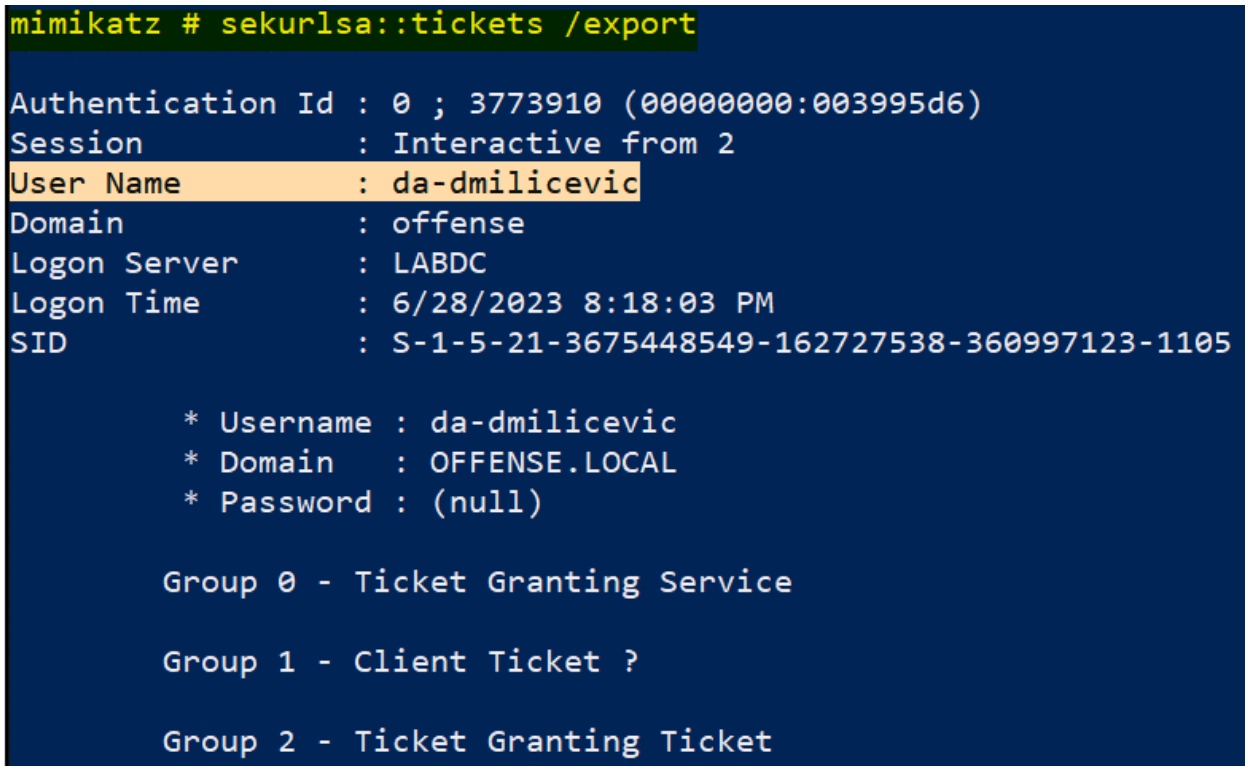
6.1 Pass-the-ticket

Slično *Pass-the-Hash* napadu, *Pass-the-Ticket* napad se svodi na izvlačenje korisničkih ulaznica iz memorije umjesto sažetaka korisničkih lozinki. Izvučene ulaznice se tada

mogu spremiti na računalo korisnika i ubacivati u procese kako bismo ih pokretali s privilegijama vlasnika ulaznice.

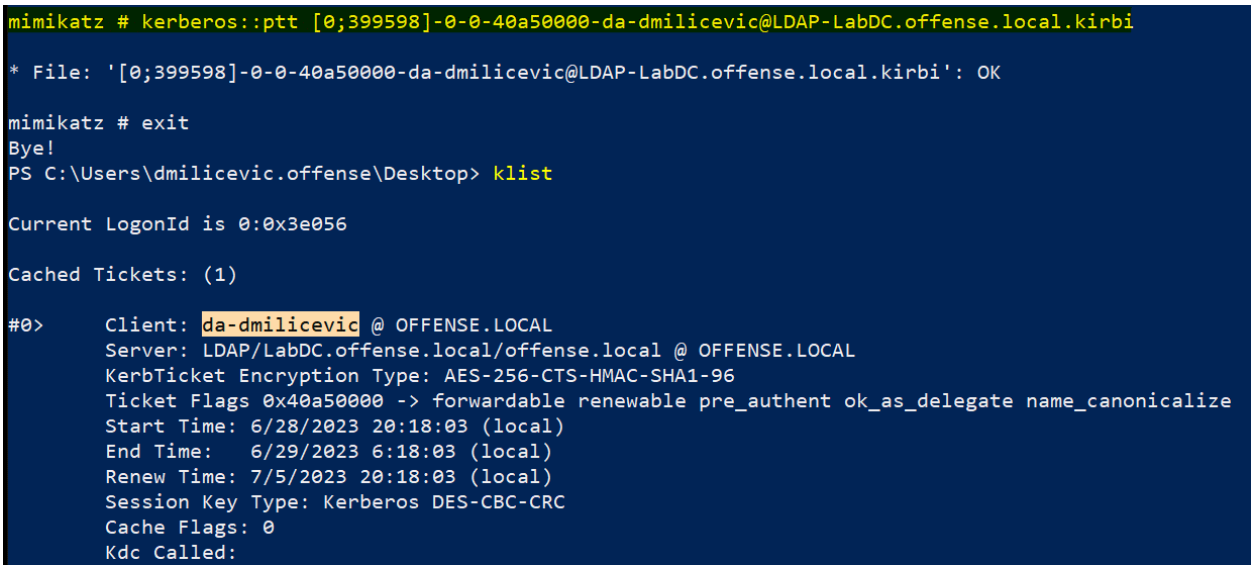
U sljedećem primjeru korišten je alat *mimikatz* kako bi se izlistale sve ulaznice koje se trenutno nalaze na žrtvinom računalu. Obzirom da smo trenutno prijavljeni kao obični korisnik *dmilicevic*, cilj nam je pronaći ulaznice korisnika s većim privilegijama, poput računa *da-dmilicevic*.

Slika 11. Ulaznice izvučene iz memorije pomoću alata mimikatz



Jednom kada izvučemo ove ulaznice, možemo ih ubrizgati u trenutno otvoreni Powershell proces kako bismo dobili privilegije korisnika *da-dmilicevic*. (Netwrix)

Slika 12. Umetanje ulaznice korisnika da-dmilicevic u otvoreni Powershell proces



6.2 Vrste Kerberos ulaznica

Iako je u prethodnom primjeru izveden običan *Pass-the-Ticket* napad gdje je iskorištena ulaznica običnog korisnika, u području PTT napada postoji nekoliko tipova ulaznica koje su od značaja – srebrne, zlatne i dijamantne ulaznice (eng. *silver, golden, diamond tickets*). Kako bi napadač uspio doći do ova 3 tipa ulaznica, prvo mora doći do NT sažetka `krbtgt` računa, računa pod kojim je pokrenut KDC. Sva 3 tipa ulaznica su iznimno slična, no razlikuju se bitnim detaljima.

Srebrne ulaznice su ulaznice koje napadač može „izgraditi“, odnosno može iskoristiti alate poput spomenutog *mimikatz* alata kako bi na temelju gotovog predloška kreirao ulaznicu za proizvoljnog korisnika. Nakon što se ulaznica izgradi, napadač će ulaznicu šifrirati NT sažetkom *krbtgt* računa te će prema KDC-u poslati šifriranu izgrađenu ulaznicu kako bi je poslužitelj uspješno dešifrirao koristeći navedeni sažetak.

Zlatne ulaznice se izgrađuju na identičan način, no razlika je u privilegijama koje su napadaču dostupne prilikom korištenja jedne odnosno druge ulaznice. Zlatne ulaznice napadačima pružaju neograničen pristup svim resursima domene – srebrne ulaznice su

ograničene, stoga napadač ne može pristupiti svakom, već određenim resursima u domeni.

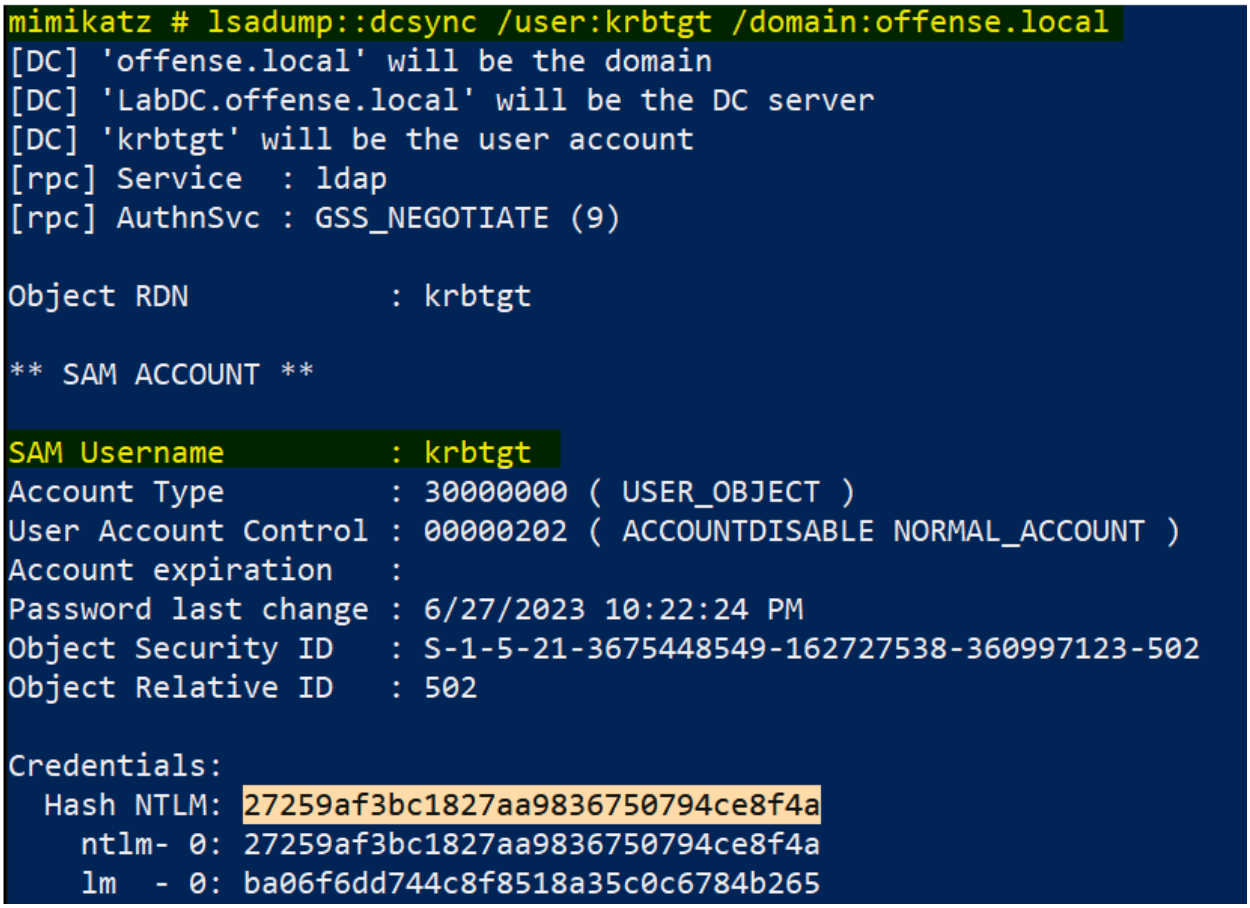
Iako je suptilan, srebrne i zlatne ulaznice imaju jedan glavni problem zbog kojeg ih je relativno lako razlikovati od normalnih ulaznica. Prisjetimo li se autentifikacijskog procesa u Kerberosu, vidljivo je da prvo *autentifikacijski poslužitelj* klijentu vraća TGT, *nakon čega* klijent taj TGT šalje TGS-u kako bi pristupio drugim resursima. To znači da svakom TGS zahtjevu (TGS-REQ) mora prethoditi zahtjev prema autentifikacijskom poslužitelju (AS-REQ). Obzirom da su srebrne i zlatne ulaznice ručno izgrađene, a nije ih izdao KDC, kod takvih ulaznica nećemo moći vidjeti povezane AS-REQ i TGS-REQ zahtjeve. Dijamantne ulaznice taj problem rješavaju korištenjem legitimnih ulaznica koje je *Domain Controller* zaista izdao u nekom trenutku u vremenu. Kada napadač uspije izvući i dešifrirati legitimnu ulaznicu, tada je može šifrirati NT sažetkom *krbtgt* računa kako bi dobio neograničen pristup svim resursima domene. Dakle, ukratko, dijamantne ulaznice su slične zlatnim ulaznicama, ali ih je znatno teže detektirati. (HackTricks)

7. DCSync napad

DCSync je tehnika izvlačenja vjerodajnica koja može dovesti do kompromitacije korisničkih vjerodajnica i, još ozbiljnije, može biti jedan od početnih koraka za stvaranje zlatne ulaznice jer prilikom izvođenja napada napadač može doći do NT sažetka *krbtgt* računa.

Kako bi se napad izvršio, napadač mora kompromitirati korisnički račun s privilegijama za repliciranje promjena direktorija. Nakon što napadač preuzme odgovarajući račun, može koristiti *Directory Replication Service Remote Protocol* (*MS-DRSR*) za repliciranje vjerodajnica i drugih podataka iz Active Directoryja. Napadač može od DC poslužitelja zatražiti početak replikacije te tako dobiti sažetke lozinki iz njegovog naknadnog odgovora. (HackTricks) Ovaj napad je moguće izvesti korištenjem *mimikatz* alata, što je vidljivo na slici iz testnog okruženja.

Slika 13. Izvlačenje NT sažetka krbtgt računa putem DCSync napada



8. Obrana od navedenih napada

U cilju obrane od ove vrste napada bitno je napraviti sigurnosni model najmanje privilegije (engl. *Principle of Least Privilege, POLP*). Ova vrsta modela ograničava opseg i ublažava utjecaj ovih napada i smanjuje sposobnost napadača da naprave eskalaciju privilegija i dopuštenja na sustavu. Ograničenja se obično daju korisnicima za prava pristupa na temelju zadataka potrebnih za njihov posao. Uklanjanje nepotrebnih administratorskih prava uvelike pomaže smanjenju prijetnje za ovu vrstu napada, ali i za druge vrste, obzirom da za izvlačenje podataka iz SAM baze napadač mora barem biti administrator računala. Također, dobra praksa je i isključivanje NTLM protokola ukoliko je to moguće obzirom na brojne ranjivosti i dostupnost modernijeg autentifikacijskog protokola u obliku Kerberosa.

9. Sažetak

Microsoft Active Directory je programsko rješenje za upravljanje resursima u organizacijskim okolinama. Temelji elementi AD sustava su njegovi korisnici, računala odnosno poslužitelji te glavni poslužitelj zvan *Domain Controller*. Unutar Active Directoryja administratorima je omogućena hijerarhijska organizacija pojedinih objekata, kao i granularno upravljanje i primjenjivanje politika nad navedenim objektima koristeći grupne politike (engl. *Group Policy Object, GPO*). Glavni strukturalni dijelovi AD sustava su pojedine organizacijske jedinice, domene i stabla odnosno šume, koji čine organiziranu cjelinu. Uz lokalnu (engl. *on-premises*) verziju Active Directoryja također postoji i modernije *cloud* okruženje zvano Azure Active Directory. Autentifikacija se unutar AD okruženja vrši koristeći dva protokola: stariji NTLM i moderniji Kerberos. Autorizacija se ne oslanja na mrežne protokole, već na ugrađene mehanizme pristupnih lista (engl. *Access Control Lists*). Zbog svojih implementacijskih mana i lokalne prirode Active Directory *on-premises* rješenja, napade na ove protokole poput *Pass-the-Ticket* i *Pass-the-Hash* je nemoguće mitigirati te se napadači uz relativno malo znanja mogu ukorijeniti duboko u mreži. Jedan od najpoznatijih alata za napad na Active Directory i njegove modele autentifikacije je *Mimikatz,* alat za izvlačenje autentifikacijskih podataka, poput sažetaka i ulaznica, iz memorije i njihovo iskorištavanje naknadno. Ključni princip mitigacije i obrane od ovakvih napada jest *Princip najmanjih ovlasti* jer je cilj napadačima maksimalno otežati put do osjetljivih podataka odnosno visokoprivilegiranih računa. Uz ovo, potrebno je voditi dobru inventuru vlastitih poslužitelja, koristiti vatrozide te sustave za detekciju napada, kao i alate za detekciju i odgovor na napad na pojedinom računalu (engl. *Endpoint Detection and Response, EDR*). Kombinacijom navedenih metodologija i alata moguće je značajno otežati napad na sustav, no nije ga moguće i spriječiti u potpunosti.

Ključne riječi: Active Directory, NTLM, Domain Controller, Kerberos, Mimikatz, Pass-The-Hash, Pass-The-Ticket, forest, domain, tree, krbtgt

10. Summary

Microsoft Active Directory is a software solution used to manage resources in an organizational environment. The foundational elements of an AD system are its users, computers or servers, and the main server dubbed the *Domain Controller*. Within Active Directory, administrators are given the leverage to organize their objects in a hierarchical manner, as well as to granularly control and enforce policies on the objects' behaviour using group policies (*Group Policy Objects, GPO*). The main structural components of an AD environment are the organizational units, domains, trees and forests which form an organized unit. Alongside the on-premises version of Active Directory, there exists a modern, cloud-based version of AD dubbed Azure Active Directory. Authentication in AD is handled by two protocols: the older NTLM and the more modern Kerberos. Authorization within an AD environment is not handled by the mentioned network protocols, but rather a model of Access Control Lists is used. Due to their implementation flaws and the nature of AD on-premises solution, attacks to these protocols are impossible to mitigate and it is possible for an attacker with little knowledge to persist deep within the network. One of the most famous toolkits for performing AD attacks and, more specifically, attacking the authentication protocols within is *Mimikatz*, a tool used to extract hashes and tickets from memory and abuse them later. The main principle for defending from these types of attacks is the *Principle of Least Privilege* model, since it is the defenders' goal to make the attacker's path to sensitive information and highly-privileged accounts as difficult as possible. Alongside this, it is necessary to have an up-to-date asset inventory, use firewalls and intrusion prevention systems, as well as per-computer Endpoint Detection and Response (EDR) agents. By combining the aforementioned methodologies and toolsets it is possible to significantly reduce the attack surface, however it is impossible to mitigate it completely.

Keywords: Active Directory, NTLM, Domain Controller, Kerberos, Mimikatz, Pass-The-Hash, Pass-The-Ticket, forest, domain, tree, krbtgt

11. Literatura

Aruba Networks. (n.d.). *Authentication, Authorization, Accounting*. Dohvaćeno iz https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm

Awati, R. (Veljača 2022). *Active Directory tree*. Dohvaćeno iz https://www.techtarget.com/searchwindowsserver/definition/Active-Directory-tree-AD-tree

Crowdstrike. (Travanj 2023). *NTLM EXPLAINED*. Dohvaćeno iz https://www.crowdstrike.com/cybersecurity-101/ntlm-windows-new-technology-lan-manager/

CyberArk. (n.d.). *Passwordless Authentication*. Dohvaćeno iz https://www.cyberark.com/what-is/passwordless-authentication/

Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. G. (2013). *Active Directory, 4th Edition.* O'Reilly.

Francis, D. (2021). *Mastering Active Directory.* Packt.

Gombos, P. (Veljača 2018). *LM, NTLM, Net-NTLMv2, oh my!* Dohvaćeno iz https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4

HackTricks. (n.d.). *HackTricks*. Dohvaćeno iz https://book.hacktricks.xyz/welcome/readme

Iyer, N. &. (2020). *Implementation of Active Directory for efficient management of networks.* Procedia Computer Science.

Krishnamoorthi, S., & Carleton, J. (Ožujak 2020). *Active Directory Holds the Keys to your Kingdom, but is it Secure?* Dohvaćeno iz https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/

Lukáš Kotlaba, S. B. (2022). *Active Directory Kerberoasting Attack: Monitoring and Detection.* Prague: Department of Information Security, Faculty of Information Technology, Czech Technical University.

Lukáš Kotlaba, S. B. (2022). *Active Directory Kerberoasting Attack: Monitoring and Detection.* Prague: Czech Technical University.

Medhi, A. (n.d.). *Windows Access Control: ACL, DACL, SACL, & ACE*. Dohvaćeno iz https://www.securew2.com/blog/windows-access-control-acl-dacl-sacl-ace

Microsoft. (Prosinac 2021). *Event Tracing for Windows (ETW)*. Dohvaćeno iz https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/event-tracing-for-windows--etw-

Microsoft. (Srpanj 2021). *Kerberos Authentication Overview*. Dohvaćeno iz https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Microsoft. (Kolovoz 2022). *Active Directory Domain Services Overview*. Dohvaćeno iz https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft. (Rujan 2022). *NTLM Overview*. Dohvaćeno iz https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview

Microsoft. (Veljača 2023). *What is Azure Active Directory?* Dohvaćeno iz https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Mokhtar, B. &. (2022). *Active Directory Attacks - Steps, Types, and Signatures.* Electronics.

Netwrix. (n.d.). *Pass the Ticket Attack*. Dohvaćeno iz https://www.netwrix.com/pass_the_ticket.html

Smith, R. (Travanj 2023). *Cyberattacks Increased 38% in 2022*. Dohvaćeno iz https://petri.com/cyberattacks-increased-38-in-2022-secure-active-directory-now/

Svidergol, B. (2023). *What is Active Directory?* Netwrix.

Warren, J. (Travanj 2022). *Overpass-The-Hash Attack: Principles and Detection*. Dohvaćeno iz https://blog.netwrix.com/2022/10/04/overpass-the-hash-attacks/